UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	
- v. -	:	05 Cr. 04 (WHP)
WILLIAM P. GENOVESE, JR., a/k/a "illwill," a/k/a "xillwillx@yahoo.com,"	:	
Defendant.	:	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

DAVID N. KELLEY
United States Attorney for the Southern
District of New York

ALEXANDER H. SOUTHWELL
THOMAS G. A. BROWN
Assistant United States Attorneys

- Of Counsel -

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	
- v. -	:	05 Cr. 04 (WHP)
WILLIAM P. GENOVESE, JR., a/k/a "illwill," a/k/a "xillwillx@yahoo.com,"	:	
Defendant.	:	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

The Government respectfully submits this memorandum of law in opposition to the motion to dismiss the Indictment on vagueness grounds filed by the defendant, William P. Genovese, Jr., a/k/a "illwill," a/k/a "xillwillx@yahoo.com" ("Genovese" or the defendant). *See* Defendant's Motion to Dismiss ("Genovese Mem."). As detailed below, Genovese fails to demonstrate that the statute is impermissibly vague or overbroad under the required high standards and his motion to dismiss should accordingly be denied.

FACTUAL BACKGROUND

On January 3, 2005 an Indictment was returned by a grand jury sitting in the Southern District of New York charging Genovese with one count of unlawfully receiving and distributing trade secrets in violation of the Economic Espionage Act, 18 U.S.C. § 1832. *United States v. Genovese*, 05 Cr. 04 (WHP). This charge stems from Genovese's obtaining and then selling, and attempting to sell, a stolen copy of the source code to two computer programs of the Microsoft Corporation ("Microsoft") from around February 2004 through around July 2004.

Both of the software programs at issue – Windows NT 4.0 and Windows 2000 – are operating systems sold by Microsoft and typically used in business environments. Operating software generally controls the allocation and usage of computer hardware resources such as memory, central processing unit (CPU) time, disk space, and peripheral devices. In essence, an operating system is the foundation on which all other programs are built. Without an operating system, a computer cannot run e-mail, word processing, or virtually any other application.

Generally speaking, software development is a labor-intensive and expensive process which first involves writing a program in the programming language of the author's choice. This human-readable code in which software developers write programs is called "source code." The source code is then "assembled" or "compiled" into machine-readable code – called "object code" – which is the format in which software is distributed and run.

Because of the investment of an enormous – indeed, possibly immeasurable – amount of developer time and expense, as well as the use of proprietary information, Microsoft asserts trade secret rights in its Windows NT 4.0 and Windows 2000 source code. Microsoft additionally owns copyrights in these products and has registered them with the United States Copyright Office under various registration numbers. Indeed, Microsoft considers the source code for its Windows products to be the "crown jewels" of the company.

Unlike Microsoft's object code, its source code for commercial products like Windows NT 4.0 and Windows 2000 is never released to the public. In fact, Microsoft closely guards the secrecy of its source code, for Windows NT 4.0 and Windows 2000, as well as its other programs. Microsoft strictly controls the distribution of its source code, and provides it to only a limited number of third parties outside the company, such as certain software developers and

government agencies. Every recipient of Microsoft's source code is required to sign a strict non-disclosure agreement and license agreement that both expressly prohibits the licensee from distributing the code to others and requires them to employ significant safeguards to protect the confidentiality of the code.

Although Windows NT 4.0 and Windows 2000 have an estimated retail value of approximately $319 per program, the value of the source code for these Windows programs is conceivably incalculable, although certainly in the hundreds of millions – if not billions – of dollars. After all, the source code for Windows is essentially the secret recipe for a product line which, according to Microsoft's 2004 10-K, generated operating income in 2004 of over $8 billion on revenues of over $11 billion. Access to the source code for Windows could allow a competitor to create lucrative competing products without investing the immense amount of developer time and expense and, perhaps more significantly, could allow hackers to more easily find holes in the operating systems which they and others can then exploit on the millions of computers running Windows operating systems (the fear of which also would increase security costs for Microsoft and all other companies and individuals running Windows programs).

Some time on or about February 12, 2004, the source code for both Windows NT 4.0 and Windows 2000 was apparently made available over some specialized areas of the Web,

including Internet Relay Chat[1] and BitTorrent[2] networks. This source code had been misappropriated from a Microsoft vendor (the "Stolen Source Code") and was unlawfully released in these areas of the Web without Microsoft's authorization.

On or about February 12, 2004 at around 6:22 p.m., Genovese, using his screen-name, "illwill,"[3] posted a message on his Web site devoted to hacking – "illmob.org" – that he had obtained a copy of the Stolen Source Code. Genovese's message also announced that he would sell the Stolen Source Code using his "FTP" server.[4] Specifically, Genovese's posting announced: "win2000 source code jacked . . . and illmob.org got a copy of it . . . im sure if you look hard you can find it or if you wanna buy it ill give you a password to my ftp."

---

[1] Internet Relay Chat – or IRC – is actually a form of communication over the Internet that allows numerous individuals to communicate through a few servers or networks of servers. IRC networks are the backbone of the IRC and are groups of IRC servers (computers and software that work like IRC switchboards, letting users connect to them by using an IRC client program) that are linked together over the Internet, enabling chat sessions to span the globe. Generally, file sharing and communication on the IRC occurs in "channels" hosted by the server networks, which are akin to the more commonly-known chat rooms. *See* Margaret Levine Young, *Internet: The Complete Reference, Millennium Edition* 324-25 (McGraw-Hill 1999).

[2] BitTorrent is a peer-to-peer file distribution protocol often used for the transfer of large volume files such as music and movie files.

[3] "Illwill" and "xillwillx@yahoo.com" were determined to be Genovese in a number of ways. Genovese, using the names "illwill" and "xxXILLWILLXxx," was convicted in Connecticut state court of eavesdropping in 2003 and sentenced to two years probation for his unauthorized access to a number of computers that he infected with viruses which allowed him to remotely access the computers. Additionally, subpoenaed records demonstrate that Genovese received the payments to "illwill" for the Stolen Source Code and that Genovese was the registered owner of a cable modem connection used to access the "xillwillx@yahoo.com" account and "illwill's" FTP server. Finally, when Genovese was arrested on these charges, he admitted to being "illwill" and "xillwillx@yahoo.com," as well as to selling the Stolen Source Code.

[4] "FTP," or File Transfer Protocol, is a protocol by which clients can transfer files to a server. An FTP server is commonly used to download files from the Internet.

As part of its efforts to track and eliminate the unauthorized dissemination of the Stolen Source Code, Microsoft retained a number of outside vendors and online security firms, one of which found Genovese's posting and on or about February 18, 2004, started corresponding with Genovese about the Stolen Source Code. The investigator ultimately purchased a copy of the Stolen Source Code for $20 from Genovese, which was downloaded from Genovese's FTP server and confirmed by Microsoft as the Stolen Source Code.

In or about July 2004, an FBI agent, acting in an undercover capacity, also obtained a copy of the Stolen Source Code from Genovese's FTP server, after the investigator made another payment to Genovese. This copy of the Stolen Source Code was also confirmed as authentic by Microsoft.

On or about November 10, 2004, Genovese was arrested at his home in Connecticut pursuant to a criminal complaint and a search was executed pursuant to a search warrant. In a post-arrest statement, Genovese admitted to possessing and having sold the Stolen Source Code and identified the computer on which the Stolen Source Code resided. Subsequent forensic examination of that computer by the FBI confirmed that Genovese possessed the Stolen Source Code.

On or about March 10, 2005, Genovese filed the instant motion to dismiss the Indictment.

ARGUMENT

Genovese urges the Court to invalidate as unconstitutional Section 1832 of Title 18, United States Code – the statute underlying the sole count of the Indictment – asserting that the statute is unconstitutionally vague under the Due Process Clause of the Constitution and unconstitutionally overbroad under the First Amendment to the Constitution. (*See* Genovese

Mem.). As set forth below, Genovese fails to demonstrate the statute's unconstitutionality under the required high standards and his motion to dismiss the Indictment should therefore be rejected.

I. THE MOTION TO DISMISS ON VAGUENESS GROUNDS SHOULD BE DENIED

A. Applicable Legal Principles

As an initial matter, although not anywhere mentioned by Genovese, a court's assessment of the constitutionality of an Act of Congress remains "the gravest and most delicate duty" that a federal court can be called upon to perform, *Blodgett v. Holden*, 275 U.S. 142, 148 (1927) (Holmes, J., concurring), since it there must pass "not on a choice made by a single judge . . . but on a considered decision of the Congress and the President." *Fullilove v. Klutznick*, 448 U.S. 448, 472-73 (1980); *see also United States v. Dennis*, 341 U.S. 494, 552 (1951) (Frankfurter, J., concurring) ("The distinction which the Founders drew between the Court's duty to pass on the power of Congress and its complementary duty not to enter directly the domain of policy is fundamental . . . Our duty to abstain from confounding policy with constitutionality demands perceptive humility as well as self-restraint in not declaring unconstitutional what in a judge's private judgment is deemed unwise and even dangerous").

In accordance with this rule of restraint in assessing a statute's constitutionality, "[i]t is common ground that [the Supreme Court], where possible, interprets congressional enactments so as to avoid raising serious constitutional questions." *Cheek v. United States*, 498 U.S. 192, 203 (1991) (citing *DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988) ("every reasonable construction must be resorted to, in order to save a statute from unconstitutionality")); *see also Public Citizen v. Dep't of Justice*, 491 U.S.

440, 465-466 (1989); *St. Martin Evangelical Lutheran Church v. South Dakota*, 451 U.S. 772, 780 (1981); *United States v. Clark*, 445 U.S. 23, 27 (1980); *Crowell v. Benson*, 285 U.S. 22, 62 and n.30 (1932). Indeed, "[t]he presumption of constitutionality which attaches to every Act of Congress is not merely a factor to be considered in evaluating success on the merits, but an equity to be considered in favor of applicants in balancing hardships." *Walters v. Nat'l Ass'n of Radiation Survivors*, 468 U.S. 1323, 1324 (1984) (Rehnquist, Circuit Justice, in chambers);[5] *see also Flemming v. Nestor*, 363 U.S. 603, 617 (1960) ("the presumption of constitutionality with which this enactment, like any other, comes to us forbids us lightly to choose that reading of the statute's setting which will invalidate it over that which will save it. (I)t is not on slight implication and vague conjecture that the legislature is to be pronounced to have transcended its powers, and its acts to be considered as void[ ]'") (quoting *Fletcher v. Peck*, 10 U.S. 87, 128 (1810)).

A claim of facial unconstitutionality in particular imposes a "heavy burden." *Sanitation & Recycling Industry v. City of New York*, 107 F.3d 985, 992 (2d Cir. 1997) (citing *Younger v. Harris*, 401 U.S. 37, 52-53 (1971)). In *United States v. Salerno*, 481 U.S. 739 (1987), the Supreme Court recounted the well settled governing principles:

> [a] facial challenge to a legislative Act is, of course, the most difficult challenge to mount successfully[.] [T]he challenger must establish that no set of circumstances exists under which the Act would be valid. The fact that the [relevant statute] might operate unconstitutionally under some conceivable set of circumstances is insufficient to render it wholly invalid, since [the Supreme Court has] not recognized an overbreadth doctrine outside the limited context of the First Amendment.

---

[5] In *Walters*, then-Justice Rehnquist granted a stay, and declined to presume the correctness, of "the action of a single District Judge declaring unconstitutional an Act of Congress that [had] been on the books for more than 120 years."

Id. at 745; *see also Ohio v. Akron Center for Reproductive Health*, 497 U.S. 502, 514 (1990); *Webster v. Reproductive Health Services*, 492 U.S. 490, 524 (1989) (O'Connor, J., concurring); *United States v. Sage*, 92 F.3d 101, 106 (2d Cir. 1996); *Giusto v. I.N.S.*, 9 F.3d 8, 10 (2d Cir. 1993).

A defendant may challenge the vagueness of a statute under the First Amendment if the conduct charged against him plainly falls within the ambit of the challenged statutory language, *see, e.g.*, *Young v. American Mini Theaters*, 427 U.S. 50, 59 (1976), but he cannot do so where the statute is subject to violation in several alternative ways and he is charged under one of the unobjectionable alternatives. *See United States v. Rahman*, 189 F.3d 88, 116 (2d Cir. 1999) (refusing to consider whether seditious conspiracy statute was unconstitutionally vague when defendant's conviction did not rest upon challenged portion of statute). Further, "speculation about possible vagueness in hypothetical situations not before the Court will not support a facial attack on a statute when it is surely valid 'in the vast majority of its intended applications.'" *Hill v. Colorado*, 530 U.S. 703, 733 (2000) (quoting *United States v. Raines*, 362 U.S. 17, 23 (1960)). Even where a litigant can pose scenarios in which the statute might encroach upon First Amendment protections, if that issue is not squarely presented by the pending prosecution, the court should not address it. "[I]f the statute's deterrent effect on legitimate expression is not both real and substantial, and if the statute is readily subject to a narrowing construction . . . the litigant is not permitted to assert the rights of third parties." *Young*, 427 U.S. at 60 (internal quotations and citation omitted); *see also United States v. Amer*, 110 F.3d 873, 878 (2d Cir. 1997) ("a challenger 'who engages in some conduct that is clearly proscribed [by the challenged statute] cannot complain of the vagueness of the law as applied to the conduct of others.")

(quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 497 (1982) (alteration in original)).

Beyond the First Amendment, a void for vagueness challenge may be brought under the Due Process Clause. Under both constitutional principles, the law is well-settled that to avoid a vagueness infirmity a criminal prohibition must "'define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.'" *Rahman*, 189 F.3d at 116 (quoting *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)); *accord Hill*, 530 U.S. at 732; *United States v. Roberts*, 363 F.3d 118, 122-23 (2d Cir. 2004); *United States v. Rybicki*, 354 F.3d 124, 129 (2d Cir. 2003) (en banc); *United States v. Sattar*, 272 F. Supp. 2d 348, 357 (S.D.N.Y. 2003).

To meet the vagueness requirements, the statute need not define the offense with "mathematical certainty," *Grayned v. City of Rockford*, 408 U.S. 104, 110 (1972), but must provide only "minimal guidelines to govern law enforcement." *Kolender*, 461 U.S. at 358 (quotation omitted). "[D]ue process does not require impossible standards of clarity." *Id.* at 361; *see also United States v. Chestaro*, 197 F.3d 600, 605 (2d Cir. 1999) ("some ambiguity in a statute's meaning is constitutionally tolerable"); *Grayned*, 408 U.S. at 110 (permissible for statutes to be marked by "flexibility and reasonable breadth, rather than meticulous specificity"). Additionally, a statute is not void for vagueness simply because its meaning may not be immediately apparent. *See, e.g.*, *Rose v. Locke*, 423 U.S. 48, 49-50 (1975); *Chestaro*, 197 F.3d at 605; *United States v. Herrera*, 584 F.2d 1137, 1149 (2d Cir. 1978). "The classification of a federal statute as void for vagueness is a significant matter," *Columbia Natural Resources, Inc. v. Tatum*, 58 F.3d 1101, 1105 (6th Cir. 1995), and the Supreme Court has accordingly "set very

high standards for invalidating a statute" on this basis, *United States v. Broussard*, 767 F. Supp. 1536, 1541 (D. Or. 1991). As the Supreme Court has explained, the void-for-vagueness doctrine "does not invalidate every statute which a reviewing court believes could have been drafted with greater precision. Many statutes will have some inherent vagueness, for [i]n most English words and phrases there lurk uncertainties." *Rose*, 423 U.S. at 49-50 (internal quotation marks and citation omitted); *accord Herrera*, 584 F.2d at 1149.

Moreover, under the Supreme Court's test, a statute is not impermissibly vague if it "conveys sufficiently definite warning as to the proscribed conduct when measured by common understanding and practices." *United States v. Petrillo*, 332 U.S. 1, 8 (1947); *accord United States v. Brunshtein*, 344 F.3d 91, 98 (2d Cir. 2003). A vagueness challenge must be evaluated on the facts as applied to the pending case, not in the abstract or based on hypotheticals. *See Sattar*, 272 F. Supp. 2d at 357 (vagueness challenge must allege that, "as applied to the conduct at issue in the criminal case, a reasonable person would not have notice that the conduct was unlawful and there are no explicit standards to determine that the specific conduct was unlawful").

To provide fair notice, the statute itself need not define all its terms, but rather "clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute." *United States v. Lanier*, 520 U.S. 259, 266 (1997); *see also Colton v. Kentucky*, 407 U.S. 104, 110 (1972) ("The root of the vagueness doctrine is a rough idea of fairness. It is not a principle designed to convert into a constitutional dilemma the practical difficulties in drawing criminal statutes both general enough to take into account a variety of human conduct and sufficiently specific to provide fair warning that certain kinds of conduct are prohibited."). Thus, as Judge

Haight has put it, "the accused is considered to have constructive knowledge of the statute's prohibition," and "judicial interpretations of the statute" at the time of the charged conduct. *United States v. Harris*, 805 F. Supp. 166, 178-79 (S.D.N.Y. 1992).

A statute passes the second part of the vagueness test so long as Congress has "establish[ed] minimal guidelines to govern law enforcement." *Kolender*, 461 U.S. at 358 (quotation omitted). "'As always, enforcement requires the exercise of some degree of police judgment.'" *Hill*, 530 U.S. at 733 (quoting *Grayned*, 408 U.S. at 114). The vagueness doctrine only requires that legislatures "set reasonably clear guidelines for law enforcement officials and triers of fact in order to prevent arbitrary and discriminatory enforcement." *Smith v. Goguen*, 415 U.S. 566, 572-73 (1974) (internal quotation and citation omitted).

Moreover, as noted above, "'every reasonable construction must be resorted to, in order to save a statute from unconstitutionality.'" *Chestaro*, 197 F.3d at 605 (quoting *Chapman v. United States*, 500 U.S. 453, 464 (1991)); *accord United States v. Harriss*, 347 U.S. 612, 618 (1954). As the Supreme Court has explained: "'The strong presumptive validity that attaches to an Act of Congress has led this Court to hold many times that statutes are not automatically invalidated as vague simply because difficulty is found in determining whether certain marginal offenses fall within their language. Indeed, we have consistently sought an interpretation which supports the constitutionality of legislation.'" *Parker v. Levy*, 417 U.S. 733, 757 (1974) (quoting *United States v. Nat'l Dairy Prods. Corp.*, 372 U.S. 29, 32-33 (1963) (citations omitted)). Thus, if a class of offenses "can be made constitutionally definite by a reasonable construction of the statute, [the courts are] under a duty to give the statute that construction." *Harriss*, 347 U.S. at 618. Additionally, as the Circuit has made clear, "[t]he claimed novelty of [a] prosecution does

not help [a defendant's] cause, for 'it is immaterial that there is no litigated fact pattern precisely on point.'" *United States v. Kinzler*, 55 F.3d 70, 74 (2d Cir. 1995) (quoting *United States v. Ingredient Tech. Corp.*, 698 F.2d 88, 96 (2d Cir. 1983)).

In determining Congress' intent in the context of a void-for-vagueness challenge, a court relies upon customary tools of statutory interpretation: most notably the language of the statute itself, *see e.g., Posters 'N' Things, Ltd. v. United States*, 511 U.S. 513, 517-19 & n.6 (1994); *United States v. Nadi*, 996 F.2d 548, 550 (2d Cir. 1993) (rejecting "as applied" challenge to Major Fraud Act), as well as the statute's legislative history, *Nadi*, 996 F.2d at 550 (deeming common sense interpretation of "value of the contract" to be "confirmed by the statute's legislative history"); *Amer*, 110 F.3d at 878 (challenge to clarity of phrase "parental rights" in International Parental Kidnaping Crime Act fails because Congress made meaning "clear in the legislative history of the Act").

B. Discussion

Genovese attacks the constitutionality of Section 1832, asserting that two different provisions of the statute are unconstitutionally vague under the Due Process Clause. (*See* Genovese Mem. at 9-19). Genovese asserts that each of these challenged clauses "failed to provide reasonable notice" of prohibited conduct, (Genovese Mem. at 9), and "encouraged arbitrary enforcement" (Genovese Mem. at 13). Genovese's arguments, however, are meritless and his constitutional attack should be rejected.

1. Section 1832

Section 1832 was enacted as part of the Economic Espionage Act of 1996 (the "EEA"). P.L. 104-294, Title I § 101(a). The statute was enacted, as the Third Circuit has described it,

"against a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage." *United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998). The EEA was motivated by Congress's concern with preserving the economic competitiveness of the nation in light of these increased threats. As the House Report accompanying the EEA explained:

> The United States produces the vast majority of the intellectual property in the world. This category of property includes patented inventions, copyrighted material, and proprietary economic information. Trade secrets, in contrast with copyrighted material and patented inventions, are information as to which owners take steps to keep confidential. The value of the information is almost entirely dependent on it being closely held. . . . For many companies this information is the keystone to their economic competitiveness. They spend many millions of dollars developing the information, take great pains and invest enormous resources to keep it secret, and expect to reap rewards from their investment. In the last few decades, intangible assets have become more and more important to the prosperity of companies. . . . Ironically, the very conditions that make this proprietary information so much more valuable make it easier to steal. Computer technology enables rapid and surreptitious duplications of the information. . . . This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft.

H. Rep. No. 104-788 at 5, 1996 U.S.C.C.A.N. 4021, 1996 WL 532685 (Sept. 16, 1996); *see also id.* ("There can be no question that the development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interests."). Indeed, the Congressional reports cited a recent study that found that "there has been a 323% increase in reported incidents [of intellectual property

theft] since a survey four years ago. . . . [and that] the potential losses for all American industry could amount to $63 billion annually." H. Rep. No. 104-788 at 6.

Federal prosecutors and law enforcement, however, were hampered in their investigation and prosecution of economic espionage cases due to the absence of any comprehensive federal statute targeting the theft of trade secrets.[6] *See* H. Rep. No. 104-788 at 6-7. Congress sought to remedy that problem in enacting the EEA. *See* S. Rep. 104-359 at 6-7, 1996 WL 497065 (Aug. 27, 1996) ("During the course of the Committee's hearings, we documented that proprietary economic information is vital to the prosperity of the American economy, that it is increasingly the target of thieves, and that our current laws are inadequate to punish people who steal the information. In a world where a nation's power is now determined as much by economic strength as by armed might, we cannot afford to neglect to protect our intellectual property. Today, a piece of information can be as valuable as a factory is to a business. The theft of that information can do more harm than if an arsonist torched that factory. But our Federal criminal laws do not recognize this and do not punish the information thief. This is an unacceptable oversight. The Industrial Espionage Act is an effort to remedy the problem."). In passing the EEA, Congress recognized "the importance of developing a systematic approach to the problem of economic espionage," H. Rep. No. 104-788 at 7, and stressed that "[o]nly by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our

---

[6] Prior to the passage of the EEA, the only federal statute directly prohibiting economic espionage was the Trade Secrets Act, 18 U.S.C. § 1905, which forbids the unauthorized disclosure of confidential government information, including trade secrets, by a government employee. This statute, however, was a misdemeanor and did not apply to private sector employees. The National Stolen Property Act, 18 U.S.C, § 2314, as well as the mail and wire fraud statutes, 18 U.S.C. §§ 1341 and 1343, were also limited in their effectiveness against economic espionage.

industrial and economic edge and thus safeguard our national security."[7] S. Rep. No. 104-359 at 11.

The House and Senate thus passed the Economic Espionage Act, and the President signed the bill into law on October 11, 1996. President Clinton, in a statement made upon signing the EEA, noted that "[t]rade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States. Economic espionage and trade secret theft threaten our Nation's national security and economic well being." 1996 WL 584924 (Oct. 11, 1996).

The EEA prohibits two principal categories of economic espionage, specifically what can loosely be termed foreign economic espionage – prohibited by 18 U.S.C. § 1831 – and private economic espionage – prohibited by 18 U.S.C. § 1832.[8] As Congress explained, "the Economic Espionage Act of l996, creates a new crime of wrongfully copying or otherwise controlling trade secrets, if done with the intent either to (1) benefit a foreign government, instrumentality, or agent, or (2) disadvantage the rightful owner of the trade secret and for the purpose of benefitting another person." H. Rep. No. 104-788 at 4.

---

[7] In passing the EEA, Congress also explicitly recognized the dangers presented by stolen computer source code and the fact that the statute covered that conduct. *See* S. Rep. 104-359 at 9 ("During its hearings, the Committee learned how an employee of Ellery Systems in Boulder, CO, transmitted that company's source code to another person in what appeared to be an attempt to appropriate the source code for his own personal use. Ellery Systems was a computer firm that supplied software technology to various government projects, primarily in NASA astrophysics activities. That theft of their source code, possibly at the behest of a foreign government, ultimately destroyed the financial viability of Ellery Systems. But all efforts to prosecute the putative thief failed because of gaps in current law.").

[8] The EEA also provides for civil actions by the Government to "obtain appropriate injunctive relief against any violation" of the statute. 18 U.S.C. § 1836(a).

Section 1831 punishes those who knowingly misappropriate, or attempt or conspire to misappropriate, trade secrets with the intent or knowledge that their offense will benefit a foreign government, foreign instrumentality, or foreign agent. 18 U.S.C. § 1831. The legislative history indicates that Section 1831 was designed to apply only when there is "evidence of foreign government sponsored or coordinated intelligence activity." 142 Cong. Rec. S12,212 (daily ed. Oct. 2, 1996).

Section 1832, the section under which the defendant is charged, is a general criminal trade secrets provision. It applies to anyone who knowingly engages in the, *inter alia*, theft, duplication, and distribution of trade secrets "with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret." 18 U.S.C. § 1832. Section 1832(a)(4) also criminalizes attempts and conspiracies as distinct offenses.

Section 1832 also contains a number of additional elements not found in Section 1831. First, a defendant charged under Section 1832 must intend to convert a trade secret "to the economic benefit of anyone other than the owner thereof," including the defendant. This "economic benefit" requirement differs from Section 1831, which provides only that the offense "benefit" a foreign government, instrumentality, or agent in any way. Therefore, Section 1832 imposes the additional limitation that the defendant intend to confer an economic benefit on the defendant or another person or entity. Another additional element in Section 1832, not found in Section 1831, is that the defendant must intend or know that the offense will injure an owner of the trade secret. The legislative history indicates that this does not require "that the prosecution

prove malice and evil intent. It merely requires that the actor knew or was aware to a practical certainty that his conduct would cause such a result." S. Rep. No. 104-359 at 15. Finally, unlike Section 1831, Section 1832 also requires that the trade secret be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[9]

The EEA defines a "trade secret" to expressly extend protection to the misappropriation of intangible information for the first time under federal law. Sub-section 1839(3) provides the applicable definition of "trade secret" as:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if–
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

18 U.S.C. § 1839(3).

This definition of "trade secrets" contained in the EEA is similar to, and was based upon, the Uniform Trade Secrets Act ("UTSA"), a model statute which permits civil actions for the misappropriation of trade secrets.[10] *See* H. Rep. 104-788 at 11 (explaining that the EEA's trade

---

[9] Section 1832 also imposes more lenient punishments than Section 1831, with a ten year statutory maximum and a $250,000 maximum fine, compared to fifteen years and $500,000 for Section 1831.

[10] For example, Section 1(4) of the UTSA states that a "trade secret" includes:

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally

secrets definition was "based largely" on the UTSA). There are, though, several significant differences that broaden the EEA's scope. First, and most importantly, the EEA protects a wider variety of technological and intangible information than current civil laws. Trade secrets under the EEA are not restricted to formulas, patterns, and compilations, but also include programs and codes, "whether tangible or intangible, and whether or how stored." 18 U.S.C. § 1839(3). Second, the EEA employs a different relevant party from whom the information must be kept secret. Under the UTSA, information classified as a trade secret cannot be generally known by businesspersons or competitors of the trade secret owner. UTSA § 1(4). The EEA, however, provides that a trade secret must not be generally known to, or readily ascertainable by, *the general public*, rather than those who can obtain economic value from the secret's disclosure or use. Finally, the EEA is specifically aimed at reaching only illicit behavior. Congress clearly limited the statute so the trade secret definition was not so broad as to prohibit lawful competition such as the use of general skills or parallel development of a similar product. *See, e.g.,* 142 Cong. Rec. S12,212 (noting that "[t]his legislation does not in any way prohibit companies, manufacturers, or inventors from using their skills, knowledge and experience to solve a problem or invent a product that they know someone else is working on").

> known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

2. The Economic Espionage Act's Definition Of "Trade Secrets" As Not "Generally Known . . . To The Public" Provides Fair Notice And Sufficient Guidance

Genovese initially asserts that the EEA is unconstitutionally vague as applied to him because the statute's definition of a trade secret as something not generally known to the public fails to provide fair notice or sufficient law enforcement guidance. (Genovese Mem. at 9-13). Specifically, Genovese argues that the definition of trade secrets in sub-section 1839(3)(B) as information not "generally known to . . . the public" is void for vagueness both because it "provides no 'relatively clear' guidance," (Genovese Mem. at 11), and because it "vested 'virtually complete discretion' in the FBI agents enlisted by Microsoft to decide whether the information Mr. Genovese had downloaded and offered for sale was 'generally known' to the public," (Genovese Mem. at 15). This constitutional challenge should be rejected because Genovese improperly focuses only on a portion of the definition of trade secret and the statute as a whole provides fair notice and guidance as to what is prohibited. Additionally, because Genovese knew – indeed, announced – the fact that the source code he was selling was stolen and valuable because not generally known, his conduct is clearly proscribed by the statute and he cannot assert the vagueness of the statute as applied to other individuals.

At the core of his argument, Genovese takes an unduly restrictive view of the definitional section, apparently believing that information can qualify as a trade secret simply if it is not "generally known" to the public. From this misapprehension, Genovese asserts that this "vague definition of 'trade secret' left Mr. Genovese with no way of knowing whether the code he stumbled across on the Internet was 'generally known' to the public by virtue of its presence in

cyberspace." (Genovese Mem. at 2). But the EEA's definition of trade secrets is actually materially different and therefore not vague as applied to Genovese.

The EEA defines trade secrets as numerous types of information, *see* 18 U.S.C. § 1839(3), that the owner reasonably tries to keep secret, *see* 18 U.S.C. § 1839(3)(A), and that "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public," 18 U.S.C. § 1839(3)(B). In other words, it is not simply information generally unknown to the public that constitutes trade secrets for purposes of the EEA but information that has actual or potential value because the public does not generally know the information or cannot obtain the information through proper means. The statute thus prohibits certain acts, such as stealing and selling, various types of information that are *valuable because not generally known or ascertainable*, not simply unknown.

Genovese's claim that because the Stolen Source Code was available over the Internet, he had "no way of knowing whether the code" was "generally known" to the public, (*see* Genovese Mem. at 2), thus falls wide of the mark. Even despite the fact that the Stolen Source Code was available over the Internet for an extremely short period of time when Genovese offered to sell it,[11] an ordinary person would still recognize that the Stolen Source Code retained value because

[11] While the Government does not contest Genovese's assertion that he is not a "first-order trade secret thief," (Genovese Mem. at 9), his implied claim that he only obtained the Stolen Source Code after it was widely available and obtained by numerous people is misleading because he in fact offered to sell the Stolen Source Code on the same day it appears to have been made available through specialized sites on the Internet. Indeed, the apparent real argument floating beneath the surface of Genovese's motion to dismiss is that the Stolen Source Code is not a trade secret, but that of course is a fact question for the jury to decide, and the Government's allegation in the Indictment that it is a trade secret must be accepted as true on a pre-trial motion to dismiss pursuant to Federal Rule of Criminal Procedure 12(b). *See, e.g., Boyce Motor Lines, Inc. v. United States*, 342 U.S. 337, 343 & n.16 (1952); *United States v.*

it was not generally known or ascertainable. Indeed, Genovese himself recognized that value at the relevant time because he offered to sell the Stolen Source Code. The EEA's definition of trade secrets as a whole – turning as it does on whether information retains value rather than simply on whether it is generally known or not – thus is readily understandable to one of ordinary intelligence. The challenged definition therefore provides fair notice as to what conduct is prohibited, especially given the strong presumption of validity and the acceptable levels of ambiguity.

This trade secrets definition also provides sufficient guidance to law enforcement. Genovese again asserts that the "generally known" definition provides "no guidance whatsoever" to law enforcement, therefore possibly authorizing or encouraging "arbitrary and discriminatory enforcement." (Genovese Mem. at 14). But the law requires only that statutes establish "minimal guidelines to govern law enforcement," *Kolender v. Lawson*, 461 U.S. 352,

---

Velastegui, 199 F.3d 590, 592 n.2 (2d Cir. 1999); *United States v. Mango*, 199 F.3d 85, 89 (2d Cir. 1999); *United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985); *United States v. Eichman*, 756 F. Supp. 143, 145-46 (S.D.N.Y. 1991).

Genovese also misleadingly cites to *DVD Copy Control Ass'n Inc. v. Bunner*, 116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185 (Cal. Ct. App. 2004), in suggesting that a trade secret loses that status after being made available on the Internet. That decision, in fact, held that dissemination over the Internet does not automatically invalidate trade secret status if the information still retains value to the owner. *DVD Copy Control Ass'n*, 116 Cal. App. 4th at 251, 10 Cal. Rptr. 3d at 192-193 ("The concern is whether the information has retained its value to the creator in spite of the publication. Publication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value.") (citation omitted). In any event, because the facts as alleged – and as will be proven at trial – demonstrate that Genovese unlawfully downloaded, duplicated, possessed, and offered to sell the Stolen Source Code almost immediately after it was made available over the specialized Internet sites, and thus before it could have been widely distributed and conceivably generally known to the public, the argument that the Stolen Source Code was not a trade secret at that time is completely meritless.

358 (1983), recognizing the fact that enforcement requires some discretion and judgment, *Hill v. Colorado*, 530 U.S. 703, 733 (2000), which the EEA plainly does. Law enforcement officers are not vested with "virtually complete discretion" in determining whether information is generally known to the public, as Genovese asserts, (Genovese Mem. at 15), because their task is simply to determine whether the information retains value because it was not generally known or ascertainable, something for which the statute provides the requisite level of guidance. Indeed, such valuation determinations are routinely made by professional law enforcement officers in a variety of contexts, such as determining that stolen property is worth more than $5,000 in assessing whether probable cause exists to believe that 18 U.S.C. § 2314 has been violated.

Moreover, the statute at issue here therefore provides materially more guidance than the state statute invalidated in *Kolender*, relied upon by Genovese, (*see* Genovese Mem. at 15), which required persons who loiter or wander on the streets to provide a "credible and reliable" identification and to account for their presence when requested by a police officer. There is thus no risk that the EEA "permit[s] 'a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections,'" *Kolender*, 461 U.S. at 358 (quoting *Smith v. Goguen*, 415 U.S. 566, 575 (1974)), the concern that animates the second prong of the vagueness doctrine.

The only reported decision addressing a vagueness challenge to the EEA, *United States v. Hsu*, 40 F. Supp. 2d 623 (E.D. Pa. 1999), rejected an attack on the same phrase Genovese challenges here. While the district court in *Hsu* expressed concerns about some ambiguities in the definitional section of the EEA, the court held that sub-section 1839(3) was not unconstitutionally vague. *Hsu*, 40 F. Supp. 2d at 630-31. Genovese tries to avoid the impact of

this decision by vainly trying to distinguish it. (*See* Genovese Mem. at 11-12). While it is true that the defendant in *Hsu* was trying to obtain the trade secrets from someone he believed to be a corrupt company insider who had told him that their actions were illegal, Genovese also knew his actions to be illegal – he was after all essentially advertising to sell property he acknowledged was stolen.[12] Genovese also focuses on the "lack of warning" as "critical" and a basis to distinguish *Hsu* where the defendant there was told by the undercover agent that their actions were illegal. (*See* Genovese Mem. at 12). While it is true that there was no explicit law enforcement warning to Genovese here, as in *Hsu*, it can hardly be said that one needs to be told that he cannot sell stolen property. *Hsu* is therefore directly applicable here and should be followed in rejecting Genovese's constitutional challenge to the EEA.

Finally, because Genovese knowingly offered to sell a stolen copy of the source code for Microsoft's Windows programs (which obviously was valuable), the statute plainly applies to him and he cannot be heard to complain about the vagueness of the statute as applied to other individuals. *See United States v. Amer*, 110 F.3d 873, 878 (2d Cir. 1997) ("a challenger who engages in some conduct that is clearly proscribed [by the challenged statute] cannot complain of the vagueness of the law as applied to the conduct of others") (internal quotation and citation omitted).

The EEA's definition of trade secrets thus provides fair notice and sufficient guidance and Genovese's vagueness challenge should be rejected.

3. The Economic Espionage Act's "Reasonable Measures" Phrase Provides Fair Notice and Sufficient Guidance

---

[12] Genovese's posting offered to sell the Stolen Source Code, which he also announced had been "jacked," a colloquial synonym to stolen.

Genovese also asserts that another aspect of the EEA's definition of trade secrets contained in sub-section 1839(3)(A) is unconstitutionally vague as applied to him. (Genovese Mem. at 15-19). Genovese argues specifically that the definitional clause requiring that the trade secret owner take "reasonable measures" to protect the secrecy of the information does not provide objective criteria by which to judge the "reasonableness" of such measures, thereby failing to provide fair notice and sufficient guidance. (*Id.*)

The EEA defines trade secrets as numerous types of information, *see* 18 U.S.C. § 1839(3), that have value due to their secrecy, *see* 18 U.S.C. § 1839(3)(B), and that "the owner thereof has taken reasonable measures to keep such information secret," 18 U.S.C. § 1839(3)(A). In other words, the owner of the trade secrets must have reasonably tried to maintain the secrecy of the information, rather than leaving it available for the taking. The legislative history to the EEA provides further guidance, explaining that:

> The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it. It is important to note, however, that an owner of this type of information need only take "reasonable" measures to protect this information. While it will be up to the court in each case to determine whether the owner's efforts to protect the information in question were reasonable under the circumstances, it is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.

H. Rep. No. 104-788 at 7.

This definition is not complicated or unclear and is readily understandable by ordinary people. The central concept behind this aspect of the definition is quite obviously that the owner

of the trade secrets take steps to safeguard the information. One need not know precisely what those steps are to know that it is unlawful to sell something of obvious value that belongs to another and that was stolen. And one need not be a company insider, as Genovese contends, (*see* Genovese Mem. at 17), to understand that a company like Microsoft would take reasonable steps to preserve the secrecy of its source code. Moreover, because Genovese in fact knew that the Stolen Source Code he offered for sale was stolen – rather than, say, voluntarily disclosed by Microsoft on their web site – he obviously knew that any safeguard measures had been circumvented and his knowledge of Microsoft's particular security measures is thus irrelevant. Again, particularly because Genovese knew the trade secrets were stolen, the statute and this definition clearly cover his conduct and his as-applied vagueness challenge should be denied. *See Amer*, 110 F.3d at 878.

Genovese particularly argues that the "reasonableness" aspect of the definition is impermissibly vague, apparently relying on *United States v. L. Cohen Grocery Co.*, 255 U.S. 81 (1921). (*See* Genovese Mem. at 16). But the mere fact that the statute employs the word reasonable – which, admittedly, does not provide an explicit objective criteria – does not render a statute unconstitutionally vague. The law recognizes as permissible some assessment of reasonableness in many other arenas, including the Fourth Amendment, U.S. Const. amend. IV (prohibiting "unreasonable searches and seizures"), the "rule of reason" in antitrust prosecutions, *see, e.g., Nash v. United States*, 229 U.S. 373, 377 (1913) (sustaining the "rule of reason" in a criminal antitrust prosecution as sufficiently definite because "the law is full of instances where a man's fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some

matter of degree. If his judgment is wrong, not only may he incur a fine or a short imprisonment . . . ; he may incur the penalty of death"), and other statutes, *see, e.g.*, 18 U.S.C. § 922(d)(8).

The district court in the Eastern District of Pennsylvania in *Hsu* also addressed, and rejected, a challenge to the "reasonable measures" phrase that Genovese attacks. *Hsu*, 40 F. Supp. 2d at 628. Specifically, the *Hsu* court held that the definition was not unconstitutionally vague simply because it used the word reasonable or unreasonable and that the defendant knew that the owner of the trade secrets at issue there had taken steps to "keep the technology to itself." *Id.* That reasoning is again directly applicable here where Genovese knew the trade secrets had been stolen and was not being voluntarily disclosed by Microsoft. The "reasonable measures" phrase therefore provides fair notice and adequate guidance and Genovese's argument that it is impermissibly vague should be rejected.

In summary, both challenged aspects of the statute plainly provide fair notice and sufficient guidance to law enforcement. Genovese has therefore not satisfied his heavy burden to overcome the presumption of validity and his motion to declare Section 1832 unconstitutional as applied to him should be denied.

II. THE MOTION TO DISMISS ON OVERBREADTH GROUNDS SHOULD BE DENIED

A. Applicable Legal Principles

Overbreadth and vagueness challenges are often closely connected, as the Supreme Court recognized in *Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 494-95 (1982), as this Court recognized in *United States v. Thompson*, 76 F.3d at 452, and as the Sixth Circuit recognized in *United States v. Jeter*, 775 F.2d 670 (6th Cir. 1985). *Hoffman Estates* taught as follows:

> In a facial challenge to the overbreadth and vagueness of a law,[ ] a court's first task is to determine whether the enactment reaches a substantial amount of constitutionally protected conduct.[ ] If it does not, then the overbreadth challenge must fail. The court should then examine the facial vagueness challenge and, assuming the enactment implicates no constitutionally protected conduct, should uphold the challenge only if the enactment is impermissibly vague in all of its applications. A plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others.

Id. at 494-95 (footnotes omitted).

Moreover, the law is well-settled that overbreadth is implicated only when a law directly regulates speech or expression. *See City Council of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 799-800 & n.19 (1984) ("the doctrine asserts that an overbroad regulation of speech or publication may be subject to facial review and invalidation"); *United States v. Salerno*, 481 U.S. 739, 745 (1987). The doctrine is highly unusual because it allows one whose own expression may permissibly be regulated to challenge a law broader than necessary to accomplish such regulation because the law's existence "may cause others not before the court to refrain from constitutionally protected speech or expression." *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973); *see also, e.g., Taxpayers for Vincent*, 466 U.S. at 798-99; *Thornhill v. Alabama*, 310 U.S. 88, 97-98 (1940).

Thus, lest this exception "swallow the general [standing] rule[,]" the Supreme Court has severely limited it: "particularly where conduct and not merely speech is involved, we believe that the overbreadth of a statute must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep.'" *Taxpayers for Vincent*, 466 U.S. at 799-800 (quoting *Broadrick*, 413 U.S. at 615); *see also CSC v. Letter Carriers*, 413 U.S. 548, 580-581 (1973). Consequently, a law that regulates speech "is unconstitutionally overbroad only if it reaches

substantially beyond the permissible scope of legislative regulation." *Taxpayers for Vincent*, 466 U.S. at 800 n.19 (emphasis added); *Hoffman Estates*, 455 U.S. at 494. Further, "[e]ven where a statute at its margins infringes on protected expression, 'facial invalidation is inappropriate if the 'remainder of the statute . . . covers a whole range of easily identifiable and constitutionally proscribable [ ] conduct.'" *Osborne v. Ohio*, 495 U.S. 103, 112 (1990) (quoting *New York v. Ferber*, 458 U.S. 747, 770 n.25 (1982)). As the Supreme Court has emphasized, the overbreadth doctrine is "strong medicine," and should be used "sparingly and only as a last resort." *Broadrick*, 413 U.S. at 613.

B. Discussion

The Economic Espionage Act plainly does not directly regulate speech, and this is dispositive. As detailed above, Section 1832 aims only a variety of *actions* – as opposed to statements – related to trade secrets, with intent to convert the trade secrets and injure the owner. Therefore, the prohibition does not affect any speech that the First Amendment protects and is not overbroad. *See Thompson*, 76 F.3d at 452 (even when dealing with a statute that directly regulated expression, i.e., "persuasion" under the obstruction of justice statute (18 U.S.C. § 1512), this Court held that because the statute only targeted persuasion that was "corrupt[ ]," it did "not proscribe lawful or constitutionally protected speech and [was] not overbroad"); *Jeter*, 775 F.2d at 678 ("ordinary criminal communication in a conspiracy . . . has been traditionally found undeserving of any First Amendment protection") & n.8 ("the activities affected by conspiracy laws . . . in the great run of situations bear no colorable claims to First Amendment protection") (quoting Note, The First Amendment Overbreadth Doctrine, 83 Harv. L. Rev. 844, 860 (1970)).

Moreover, a prohibition against the theft or unlawful distribution of trade secrets, like the "prohibition against corrupt [verbal] acts" found by this Court in *Thompson* and the Sixth Circuit in *Jeter*, "is clearly limited to . . . constitutionally unprotected and purportedly illicit activity.'" *Thompson*, 76 F.3d at 452 (quoting *Jeter*, 775 F.2d at 679). This is especially so because of the additional limitations placed on the statute's reach imposed by the requirements that a defendant act with intent to convert the trade secret to the economic benefit of someone other than the owner and that a defendant act with intent or knowledge that the offense will injure the owner. Thus, because no speech is regulated by the EEA and the statute is limited to unprotected and illicit activity, Genovese's facial challenge to the statute should be rejected.

Despite the fact that the EEA does not regulate speech, Genovese contends that the Stolen Source Code is protected speech because computer code has been held to be speech protected by the First Amendment and it conveys information. (*See* Genovese Mem. at 24-25). But this argument misses the point that the EEA criminalizes the disclosure and theft of trade secrets, rather than the content of the information. Therefore no speech is regulated and the facial challenge is meritless. Indeed, to carry Genovese's argument to its logical conclusion, any restriction on the disclosure of information, such as the general requirement that one pay royalties for using someone else's artistic work, would be unconstitutionally overbroad.

Therefore, because Section 1832 reaches no protected speech at all, let alone so significant a degree as to be considered "substantial" when compared to the statute's legitimate scope, Genovese's overbreadth claim is unavailing.

CONCLUSION

For the foregoing reasons, Genovese's motion to dismiss the Indictment on the basis that Section 1832 is unconstitutionally vague and overbroad should be denied.

Dated: New York, New York
April 15, 2005

Respectfully submitted,

DAVID N. KELLEY
United States Attorney
Southern District of New York

By: /s/
ALEXANDER H. SOUTHWELL
THOMAS G. A. BROWN
Assistant United States Attorneys
(212) 637-2417 / 2194